LotDepot: A Data Depot with Entry Correctness from Probability Amplification

Wenbo MAO and Wenxiang WANG
DaoliCloud
Beijing, China
daolicloud.com

October 18, 2021

Abstract

LotDepot is a permissionless blockchain for a scalable, decentralized, and secure database (DB), in particular suiting an open ledger usecase which must quickly reject any accounting error, e.g., double spending. Its block finding algorithm is by way of noisy drawing lots to select a lucky block from many contenders. Let the lucky block finder record in its lucky block, not only a payload item containing DB entries as all blockchains conventionally do, but also the public-key identities of a lot of not-so-lucky block finders, to name this unconventional item of blockchain data "payroll". Let only the payroll nodes, i.e., those not-so-lucky block finders, announce accounting correctness validation outcome for DB entries input by the lucky block's payload item. By controlling the volume of the payroll nodes under a non-spam level, the accounting correctness validation dissemination from the payroll nodes can be in good order to propagate and influence through out the forwarding network. Also because subsequent payroll nodes can never be used up, any correct accounting outcome from them will always enter the DB, in fact very quickly since the payroll nodes work for an incentive. Thus, this unconventional design of blockchain payroll functions as *probability amplification* for the block extending algorithm which is in fact a randomized probabilistic (RP) algorithm. The work of LotDepot manifests for the first time the so-far having been ignored fact: The decision problem for a public blockchain's accounting correctness is in the Zero-sided-error Probabilistic Polynomial (ZPP) time class, i.e., a public blockchain should be *always fast and always correct*. The work of LotDepot makes a knowledge advance for the blockchain consensus layer algorithms status quo, including known slowness with the so-called Proofs-of-Work (PoW)

consensus model, and known impossible distributed fungibility between an accounting error and an amount of security deposit to "slash" with the so-called Proofs-of-Stake (PoS) (non-)consensus model.

In addition to improving the permissionless blockchain technology, LotDepot also lines up payroll nodes for an unbound volume of IT resources to organize an open cloud and host general-purpose peer-to-peer applications.

Key Words and Phrases: Green, Quick and Scalable Permissionless Blockchain. Blockchain Consensus Layer Security. Amplification of Success Probability for Blockchain Ledger Correctness. Index Partitioned UTXO Sets. P2P Cloud.

1 Introduction

Bitcoin began the era of open source P2P money and inspired the blockchain technology. LotDepot taps the potential of the blockchain technology to contruct an open and secure database for applications of secure and low-cost P2P money and computing. We began our work presentation with discussions on a number of issues in the blockchain area of study.

Nondeterminism with Proofs-of-Work An in-the-spotlight issue for permissionless blockchains is about a phenomenally poor scalability. Bitcoin is a notoriously slow and energy wasteful payment instrument. Its block extending algorithm, so-called "Proofs-of-Work (PoW) mining", has the following purposely designed low bandwidth properties. Property 1: Time for finding a block is prolonged to many minutes. Property 2: Data size for an accounting payload in a block is limited to a low megabyte level. Property 3: Upon spotting an accounting error, let miners fork the chain at the error spot and race; one correct racer shall eventually win. Property 1 is for lowering the probability of mining race condition. Property 2 is for highering the probability of accounting correctness. Property 3 is for exceptions covering error or no-error race conditions: the longest fork to win the race is a simple fail-proof design. With these properties Bitcoin does work correctly, however has a very poor scalability. After Bitcoin, many proposals for improving permissionless blockchain appeared. Formulations vary, e.g., an eased version of GHOST for Ethereum, however none has gone beyond Bitcoin's idea of sorting out accounting error during blockchain extending, with no success unfortunately. We would like to attribute the root cause of slowness and poor scalability with PoW blockchains to nondeterminism for deciding accounting correctness. A PoW blockchain needs some uncertainly long wait for an accounting entry to become certain. The slowness and poor scalability of PoW blockchains limit not only the usages for a P2P money, but also the usefulness of an open DB for third party applications.

Between Accounting Error and Stake In frustration of PoW blockchains having no scalability, the blockchain industry has emerged a so-called "Proofs-of-Stake" (PoS) blocking model. In the PoS blocking model, a blockchain participant wishing to generate blocks must submit an amount of money's worth asset, called security deposit, to a (centralized?) blockchain management body. The more amount of the security deposit a participant submit, the more chance for its turn to generate a block. As an academic idea, the security deposit is for punitive confiscation or destroy (in PoS programmers' jargon,"money slashing") in case when a block generator is found having caused an accounting error. We regard the move from PoW to PoS as a way-too-easy giving up: it relinquishes the astonishing manifestation of Bitcoin that a permissionless autonomy can have good congruence, and surrenders to the old world order of wealth controlling the means of production. "Ethereum 2.0" would be the brightest of such a u-turn to take place in a near future of writing this paper.

Money slashing in PoS is an idea easier said than done. Since a blockchain runs over a distributed network, money slashing need to be an action of a collective consensus. As parties involved in reaching such a consensus are located in various corners of the network, input to each of them is an in-hearing message and varies inconsistently for various parties including attackers. For a network distributed algorithm inputting inconsistent in-hearing/attacking messages to output a money slashing consensus, this is a well-known academic conclusion named "FLP Impossibility". Even for money slashing to be executed manually by the programmers, they would need a fungibility exchange rate between an "error" and money amount to slash. A number of PoS blockchains, e.g., Peercoin, Myriad, Blackcoin, VeriCoin, NXT, Algorand, have appeared. They serve pre-echos for new PoS blockchains to come, e.g., Ethereum 2.0, Solana, for the blockchain industry to try-and-error learn the PoS idea. Given that the PoS idea is by way of business arrangement to avoid poor scalability of PoW, a for-profit business participant in a PoS blockchain will have to discover a profit margin to compensate the risk of its security deposit to be mistakenly slashed. The higher the risk a participant to experience, the higher the profitable margin to discover. The discovered profit margin will certainly translate to fees over to the blockchain users.

Rethinking Blockchain Security The discussions above confess an unsatisfactory status quo on how public blockchains reach consensus: it is all about bid for power. Bid for power in PoW is by way of realtime showdown of hashrate possession. It takes a long time to demonstrate a clear difference in hashrate possession. The slowness of realtime power showdown limits PoW blockchains' usefulness for not only P2P money but also third party applications. Bid for power in PoS is brutally simpler: the-richer-the-stronger control. However, a consensus algorithm for an accounting "error" matching a money amount to slash remains an idea easier said than done. Long term equitability of return-on-stake is yet to be discovered by both the business

sector and the users' satisfactory on service fees. Only time will tell.

Bid for power, as the status quo means to secure today's PoW and PoS blockchains, has a strong centralization taste. Rethinking blockchain security by avoiding any idea of centralization, an observation is shaping up from a P2P network's property of relying on forwarding/propagation/influencing to transmit messages. If we can formulate some distributed algorithm for messages of quality content to travel afar and widely through a P2P forwarding/propagation network and thereby make stronger influences, then it can be intuitively expected that such an algorithm has merit of decentralization. The intuition makes sense since far and wide propagation of quality content needs approval by a majority of the participants in a P2P forwarding/propagation network.

Propagation of Influence by Quality of Content Let a blockchain's accounting algorithm be very easy, so easy that a low-end computer such as a smartphone or an IoT device can quickly give a correct/error answer on a bundle of accounting requests. Such an accounting algorithm can base a truly decentralized security foundation for the blockchain in a P2P propagation network. Now suppose the worst case attacking scenario: let a computationally powerful and/or monetarily resourceful participant in this blockchain send out an error accounting result to the network. Since the attacking message can be quickly judged invalid by a majority of the network participants and dropped from propagation, it cannot be written into the blockchain, regardless of how computationally powerful or monetarily resourceful the attacker is. This propagation-of-influence-by-quality-of-content notion of blockchain security can also resist a so-called "Nothing-at-Stake" attack, or a so-called "Sybil" attack.

The remaining job for us is to devise a blockchain and its accounting algorithm, for the former to be able to attract a large number of low-end computer holders to participate in a propagation-of-influence-by-quality-of-content game, and for the latter to be able to quickly validate an accounting result by a majority of the game participants.

Decoupling Between Accounting and Block Extending LotDepot's approach to an easy accounting validation is to decouple the job of accounting away from that of blockchain extending. Let permissionless participants race to generate blocks noisily. Let a draw-on-lots race winner document, not only payload data as all blockchains to date conventionally do, but also the public keys of many (of course a non-spam volume of) the race losers. This unconventional part of the block data is named *payroll*. The block address, i.e., the chain height, of the race winner's block specifies a number of accounting requests in the payload for the payroll nodes to exame and disseminate the correct ones to the network for a ledger entry influence. Thus, the already lineup payroll nodes are specifically and accountably assigned to process the *deterministic in-*

writing payload rather than to do some *nondeterministic in-hearing* ones. In speaking of "deterministic in-writing", we mean for all distributed nodes in the network to process whatever the lucky race winner has heard and written in the block payload it generates. In speaking of "nondeterministic in-hearing", we mean the nature of the input to the cases in the current status-quo blockchain accounting algorithms, or to all Byzantine Fault Tolerance (BFT) discussion algorithms; such in-hearing input to distributed nodes in various corners of the network is non-deterministic and inconsistent, and can cause these nodes in uncertainly long discussions, more likely for them to disagree on, various messages individually heard by each of the nodes. The nondeterministic in-hearing input computation, discussion or disagreement has unfortunately been responsible for slowness with PoW blockchains, for the reason why BFT has the FLP-Impossibility, and perhaps will also render a money-slashing algorithm in a future PoS blockchain to be executed manually.

Of course a deterministic in-writing payload may contain errors, especially considering that the payload is composed in a race. However, for the in-writing specified, accountable and non-spam volume of the payroll nodes to process the deterministic in-writing payload, their computational influence in the propagation network is easily error-free. In speaking of "easily error-free", we mean that any error caused by a network imperfection is easily distinguishable from that of a malicious attack, even considering the attacker being the draw winner or some payroll nodes. Any attacking traffic can be easily dropped during the P2P propagation and cannot cause an errorsome infludne to the accounting.

Why and How Easy for Accounting Validation The explicit assignment of the deterministic payload data to a specific set of accountable payroll nodes means that the accounting requests, i.e., the user transactions, in the assigned block payload can be immutably indexed to the block address right at the time of the block extending. Being able to index the accounting requests enables a clear partition on the resultant ledger set. Partitioned ledger subsets can be created and DB-maintained in a sorted order. The current Bitcoin's linear-space complexity accounting correctness tracking algorithm on input a very large and ever growing size UTXO set, now in LotDepot, is drastically reduced to a logarithmic complexity on input much smaller indexed subsets. With the much eased DB-management for the partitioned smaller ledger sets, the job of accounting, and the distributed job of correctness validation on an accounting result in propagation, in the LotDepot blockchain can indeed be quickly executed by a majority of client quality devices.